UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,474	09/30/2003	Klimenty Vainstein	2222.5450000	7534

26111 7590 10/13/2009

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
10/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/676,474	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's submission for RCE filed on amendment filed on 7/28/2009 has been entered. In the amendment filed on 6/29/2009, applicant has amended claims 1, 2, 11, 12, 14, 18-24, and 26-28. Currently claims 1-28 are pending in this application.

Response to Arguments

1. Applicant's arguments filed 6/29/2009 have been fully considered but they are not persuasive following reasons:

- Applicant argues that, "Serbinis discusses how "[s]tates for a document instance include "pending," "active," "archived," "canceled" and "deleted"" (Serbinis, col. 7, ln. 67 - col. 8, ln. 1). However, Serbinis describes that "[d]ocument instances are marked "canceled" when an Authorized User (typically the Originator) forces a document to expire before the expiration time" and that **"[c]anceled document instances then are treated like archived document instances"** (Serbinis, col. 8, lns. 26-31) (emphasis added). Even assuming arguendo that Serbinis' document instance states are analogous to the process-driven security policy states recited in claim 1, each of Serbinis' document instance states clearly do not have distinct access restrictions, as recited in claim 1. As recited in claim 1, "the process- driven security policy includes a plurality of different states and transition rules", "each of the states is associated with one or more access restrictions", "each

of the states has distinct access restrictions", and "the transition rules specify circumstances under which a secured document is to transition from one state to another". In contrast, in Serbinis' system, at least two of the document instance states (e.g., "canceled" and "archived") are treated identically (Serbinis, col. 8, lns. 26-31). Therefore, the canceled and archived document instance states in Serbinis are not different states wherein each of the states has distinct access restrictions, as recited in claim 1."

- Examiner would like to point out that due to amendment made to the claim language, examiner is now equating only "pending", "active", and "deleted" states to the claimed plurality of different states. When only "pending", "active", and "deleted" states are treated to be equivalent to the claimed "plurality of different states", Serbinis still anticipate the claim language because "pending", "active", and "deleted" do have distinct access restrictions (see, Column 8, lines 5-26). Therefore, Serbinis still discloses "wherein the process-driven security policy includes a plurality of different states and transition rules, and wherein each of the states is associated with one or more access restrictions, and wherein each of the states has distinct access restrictions".
- Applicant further argues that, "Moreover, although Serbinis describes that "[d]ocument instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active"" (Serbinis, col. 8, lns. 5-8), Applicants submit that

triggering a change from a pending state to an active state based solely on time is not analogous to transition rules that specify circumstances under which a secured document is to transition from one state to another, as recited in claim 1. A non-limiting example of transition rules is provided in the instant specification at, for example paragraph [0049], where it is disclosed that in an embodiment, a "file can transition between the various states of the process-driven security policy 100 in a controlled manner", "[o]ften, the process-driven security policy 100 defines the transitions that are permissible", "the state transitions are event-driven", and "some events can be triggered or initiated by user or administrator interaction."

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a "file can transition between the various states of the process-driven security policy 100 in a controlled manner", "[o]ften, the process-driven security policy 100 defines the transitions that are permissible", "the state transitions are event-driven", and "some events can be triggered or initiated by user or administrator interaction") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Also note that applicant's argument that "triggering a change from a pending state to an active state based solely on time is not analogous to transition

rules that specify circumstances under which a secured document is to transition from one state to another" is not found persuasive because claim only defines transition rules to specify circumstances under which a secured document is to transition from one state to another. Examiner asserts that triggering a change based on a time is in fact "circumstance" under which a secured document is to transition from one state to another. Claim language does not prohibit using time as a circumstance under which a secured document is to transition from one state to another. Therefore, Serbinis still discloses "process- driven security policy including a plurality of different states and transition rules, wherein the transition rules specify circumstances under which a secured document is to transition from one state to another". Therefore, the rejection is maintained.

- Applicant further argues that, "Further, Serbinis fails to disclose an access manager configured to enable a processor to access a process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy, as recited in claim 1. The Examiner asserts that the above-recited access manager features recited in claim 1 are disclosed by Serbinis in passages in columns 8-10 (See Office Action, pages 6 and 7). Applicants respectfully disagree with the Examiner's contention. Although Serbinis may describe that an "Authorized User may

then request retrieval of the document" from a data store "and any automatic filtering, or filtering selected by the Authorized User, may be performed during the document download process" before "[t]he document is then downloaded to the Authorized User" (Serbinis, col. 9, ln. 66-col. 10, ln. 4), Serbinis fails to teach or suggest the above-noted features of the access manager recited in claim 1."

- Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant simply stated that "Serbinis fails to teach or suggest the above-noted features of the access manager recited in claim 1" without giving any reasoning as to how the claim language is different then passages provided by examiner. Furthermore, Serbinis discloses access manager configured to enable a processor to access a process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20. Column 9, line 64-Column 10 line 5 describing the authentication process and Column 8, lines 1-20, discloses a "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all

Authorized Users, so the authentication step determine the access based on policy state associated therewith at the time access is requested and the corresponding one or more access restriction thereof for the process-driven security policy). Therefore, Serbinis discloses all the limitations argued above and the rejection is maintained.

- Regarding Claim 14 and 27, applicant argues that, "Moreover, while Serbinis may generally describe "a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time" (Serbinis, col. 7, lns. 63-67), Serbinis does not teach or suggest automatically transitioning from the former state to the subsequent state of the security-policy state machine upon determining that an event causes the state transition, as recited in claims 14 and 27. In Serbinis' DMS system, a document instance transitions based upon an "expiry date" (Serbinis, col. 7, lns. 32-37). Document instance states in Serbinis only transition "when the expiration time is reached", "after a pre\-determined amount of time", or "when an Authorized User (typically the Originator) forces a document to expire before the expiration time" (Serbinis, col. 8, lns. 12-29). In contrast, claims 14 and 27 recite, using respective language, automatically transitioning a secured document from a former state to a subsequent state of the security-policy state machine upon determining that a detected event causes the state transition. In contrast to the above-noted distinguishing features of claims 14 and 27, Serbinis' DMS system

modifies the state of a document instance based only on the document's current state, the active date/time, and expiration date/time (the expiry date) (Serbinis, col. 7, lns. 32-37 and 63-67)."

- Examiner respectfully disagrees and would like to point out that Serbinis discloses automatically transitioning from the former state to the subsequent state of the security- policy state machine upon determining that an event causes the state transition (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time.", Note: examiner is equating the active date/time and expiration date/time as the claimed events that causes the state transition). Applicant's argument that claim require the state transition based on an detected event which is not same as state transition based on the active date/time and expiration date/time is not found persuasive because active date/time and expiration date/time can reasonably interpreted as an event that causes the state transition. Claim language does not prohibit using time as a circumstance under which a secured document is to transition from one state to another. Therefore, Serbinis discloses above argues limitation and the rejection is maintained.

Note: Applicant relied upon similar argument for the rest of the independent and dependent claim rejection. Arguments discussed above are not found persuasive. As a result rejection of all other independent claims and dependent claims are also maintained for the same rational.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9, 11, 13-18 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Serbinis et al. (US 6,584,466 B1), hereinafter "Serbinis".

Regarding **Claim 1**, Serbinis discloses a document security system for restricting access to secured documents (See Fig. 1-5) comprising:

a processor (see, Fig. 1B, numerals 20 A, 20 B);

a policy module configured to enable the processor to store at least one process-driven security policy (see, Column 7, lines 63-67, "document state process") on a

computer readable storage medium, wherein the process-driven security policy includes a plurality of different states (see, Column 7 line 67- Column 8, line 4, "pending," "active," and "deleted" states, Note: examiner is equating only pending, active and deleted states to the claimed plurality of different states) and transition rules (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.""), wherein each of the states is associated with one or more access restrictions, and wherein each of the states has distinct access restrictions (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.") and wherein the transition rules specify circumstances under which a secured document is to transition from one state to another (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active.").

an access manager module configured to enable the processor to access the process-driven security policy and determine whether access to a secured document is permitted by a requestor based on the policy state associated therewith at the time access is requested and the corresponding one or more access restrictions thereof for the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20, Column 9, line 64- Column 10 line 5 describing the authentication process and Column 8, lines 1-20, discloses a "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all

Authorized Users, so the authentication step determine the access based on policy state associated therewith at the time access is requested and the corresponding one or more access restriction thereof for the process-driven security policy).

Regarding **Claim 2,** the rejection of claim 1 is incorporated and Serbinis further discloses that the one or more access restrictions for the secured document are automatically changed if the state of the process-driven security policy for the secured document changes (see Column 7, lines 63-67).

Regarding **Claim 3,** the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to automatically transition from one state to another (see, Column 7, lines 63-67).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and Serbinis further discloses that the events are internal or external events with respect to the document security system (See, Column 7, lines 63-67).

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Serbinis further discloses that at least one of the events is an external event from a document management system (see Column 8, lines 26-30).

Regarding **Claim 6**, the rejection of claim 1 is incorporated and Serbinis further discloses that one or more of the corresponding one or more access restrictions for access to the secured document remain intact when the state of the process-driven security policy for the secured document changes (see paragraph 0123)

Regarding **Claim 7**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state and a third state and second event that causes transition from the second state to a third state (see, Column 8, lines 1-20).

Regarding **Claim 8**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy to automatically transition from one state to another (see Column 7, lines 63-67).

wherein the process-driven security policy includes at least a first state and a second state, and wherein a first event causes transition from the first state to the second state (see Column 8, lines 1-20).

Regarding **Claim 9**, the rejection of claim 1 is incorporated and Serbinis further discloses that transition rules are based on events (see Column 8, lines 1-20).

Regarding **Claim 11**, the rejection of claim 1 is incorporated and Serbinis further discloses that events cause the state of the process-driven security policy for the secured document to transition from a previous state to a current state, and wherein the secured document is modified if the process-driven security policy for the secured document transitions from the previous state to the current state (see Column 7, lines 63-67).

Regarding **Claim 13**, the rejection of claim 11 is incorporated and Serbinis further discloses when permitted, access to the secured document is available at a client machine (see, Column 10, lines 3-4).

Regarding **Claims 14 and 27**, Serbinis discloses a method and a corresponding software program for transitioning at least one secured document through a security-policy state machine having a plurality of different states (see, Column 7 line 67-Column 8, line 4, "pending," "active," and "deleted" states, Note: examiner is equating only pending, active and deleted states to the claimed plurality of different states), each of the plurality of states having distinct access restrictions (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users."), the method comprising:

receiving an event (see, Column 7, lines 63-67, "the active date/time, and expiration date/time")

determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process")

automatically transitioning from the former state to the subsequent state of the security-policy state machine if the determining determines that the event causes the state transition (see, Column 7, lines 63-67, "In a preferred embodiment, documents stored in the DMS system are monitored by a document state process that

automatically modifies the state of a document instance based on its current state, the active date/time, and expiration date/time.")

Regarding **Claim 15**, the rejection of claim 14 is incorporated and Serbinis further discloses the security-policy state machine implements a process-driven security policy, and wherein each state of the security-policy state machine has different access restrictions (see Column 8, lines 1-20).

Regarding **Claim 16**, the rejection of claim 14 is incorporated and Serbinis further discloses each of the states of the security-policy state machine have different access policies (see Column 8, lines 1-20).

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Serbinis further discloses the security-policy state machine is provided as part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system (See, Column 8, lines 1-20 and Column 9, line 63- Column 10, line 5)

Regarding **Claim 18**, the rejection of claim 14 is incorporated and Serbinis further discloses wherein the transitioning comprises modifying the secured document to reflect the subsequent state of the security-policy state machine (see Column 7, lines 63-67).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Li et al. (US 2004/0193912 A1), hereinafter Li.

Regarding **Claim 10**, the rejection of claim 9 is incorporated and Serbinis does not teach that the transition rules are written in XML.

However, Smith et al. in the same field of endeavor of network security discloses writing security policies in XML format (Paragraph 0014, "In one embodiment of the present invention, the security policies are stored in a relational database in a native Extensible Markup Language (XML) format")

Therefor, it would have been obvious at the time the invention was made to one of ordinary skill in the art to write the transition rules of Serbinis in XML format as taught by Li because XML is a text-based and platform independent, as a result policy server would be able to enforce and distribute the policies to all client having any type of operating system platform.

Claims 12, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Dilkie et al. (US 6341164), hereinafter "Dilkie".

Regarding **Claim 12**, the rejection of claim 11 is incorporated and Serbinis further discloses that the secured document includes at least a security information portion (see, Column 9, lines 21-25 and Column 7, lines 33-40) and an encrypted data portion (see, Column 11, lines 7-10) and further discloses transitioning secure document from the previous state to the current state (see, Column 7, lines 63-67).

Serbinis discloses encrypting document with the session key and require the retriever of the document to provide the same key to decrypt the documents. However, Serbinis does not explicitly discloses the security information portion including at least an encrypted key, and the key being encrypted is decrypted in order to decrypt the encrypted data portion and wherein if the process-driven security policy for the secured document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state.

However, Dilkie discloses security information portion including at least an encrypted key (Column 4 lines 1-3, "A cryptographic key package may include, for example, a symmetric encryption key wrapped, or encrypted, with an asymmetric encryption key, such as a recipient's public key..."), and the key being encrypted is decrypted in order to decrypt the encrypted data portion (Column 7 lines 46-50, "The corresponding private key (for example, signing key) is used to unwrap the cryptographic key package to recover a message encryption key as known in the art. The system may re-encrypt the key package with a different asymmetric key and/or algorithm as shown in block 409. The analyzer 103 may then decrypt the message data in any suitable manner using the message encryption key as shown in block 410".) and wherein when, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the modified document (Column 7 lines 46-50, "The corresponding private key (for example, signing key) is used to unwrap the cryptographic key package to recover a message encryption

key as known in the art. The system may re-encrypt the key package with a different asymmetric key and/or algorithm as shown in block 409. The analyzer 103 may then decrypt the message data in any suitable manner using the message encryption key as shown in block 410".).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to improve the encryption system of Serbinis by encrypting the session key using the public key as taught by Dikkie because it provides extra security and provide secure session key exchange. It would have been further obvious to modify the secured document of Serbinis by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis so that system would need to re-encrypt the "header without re-encrypting the file itself, thereby only changing the wrapping on the header key" (Dilkie, column 8, lines 19-21)

Regarding **Claim 19**, the rejection of claim 14 is incorporated and Serbinis does not teach retrieving an encrypted file key from the secured document; decrypting, if permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key; subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; decrypting, if permitted, the encrypted file key to yield a file key;

subsequently encrypting the file key and storing the secured document, (column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored") the secured document including at least an encrypted data portion (column 4, lines 7-8, "the encrypted message data with the header data") and the subsequently encrypted file key (Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis to re-encrypt the "*header without re-encrypting the file itself, thereby only changing the wrapping on the header key*" (Dilkie, column 8, lines 19-21)

Regarding **Claim 20**, the rejection of claim 14 is incorporated and Serbinis does not teach a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine;

subsequently encrypting the file key in accordance with the public state key; and storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

However, Dilkie discloses a method of retrieving an encrypted file key from the secured document; obtaining a private state key associated with the former state of the security-policy state machine; decrypting the encrypted file key using the private file key; obtaining a public state key associated with the subsequent state of the security-policy state machine; subsequently encrypting the file key in accordance with the public state key; and storing the secured document, (column 8, lines 11-18, "incoming message is encrypted under algorithm X with symmetric key Y wrapped (encrypted) with asymmetric key Z, the system may decrypt asymmetrically to recover the symmetric key Y, and re-encrypt the symmetric key Y with a different asymmetric key Z' and replace the previous cryptographic key package with the new re-encrypted key data forming a new cryptographic key package in the header. The message data with the new cryptographic key package may then be stored") the secured document including at least an encrypted data portion (column 4, lines 7-8, "the encrypted message data with the header data") and the subsequently encrypted file key (Column 3, lines 62-63, "The cryptographic key package information is preferably contained as header data")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to modify the secured document by decrypting the encrypted key and then re-encrypting the key as taught by Dilkie when document transit from one state to another state as taught by Serbinis to re-encrypt the *"header without re-*

encrypting the file itself, thereby only changing the wrapping on the header key" (column 8, lines 19-21)

Claims 21-26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serbinis in view of Leser et al. (US 2005/0028006 A1), hereinafter "Leser".

Regarding **Claims 21 and 28**, Serbinis discloses a method and corresponding computer program for imposing access restrictions on electronic documents, the method comprising:

providing at least one process-driven security policy at a server computer, wherein the process-driven security policy is associated with a plurality of different states (see Column 8, lines 1-20, "Document instances with a "pending" state have an active date/time that specifies the time at which the state of the document instance should be changed to "active."") and wherein each of the states has distinct access restriction (see, Column 8, lines 1-20, "A "pending" document is not available to anyone except the Originator. Document instances marked "active" are accessible by all Authorized Users.");

Serbinis does not disclose: providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document.

Leser discloses providing a reference to the process-driven security policy to client computer, the reference referring to the process-driven security policy resident on the server computer and associating the reference to an electronic document (see,

Paragraph 0208, Note: Paragraph 0208 is fully supported by the provisional application at least at Page 32, lines 3-10).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to cache security-policy of the system of Serbinis into the user's computers thereby enabling them to generate and or use protected document while they are off-line.

The combination of Serbinis and Leser further discloses

transitioning the process-driven security policy from one state to a current state (see, Column 8, lines 1-20); and

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy (see, Column 9, line 64- Column 10 line 5 and also Column 8, lines 1-20), the current state being informed to the server computer by sending the reference to the server computer (see, Leser, Paragraph 0029, Note: Paragraph 0029 is fully supported by the provisional application at least at Page 9, lines 1-4).

Regarding **Claim 22**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the transitioning is automatically performed based on events (see, Column 7, lines 63-67).

Regarding **Claim 23**, the rejection of claim 22 is incorporated and Serbinis further discloses wherein the transitioning is performed at the server computer (see, Column 7, lines 63-67).

Regarding **Claim 24**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the associating associates the reference to a group of documents (See, Column 7, lines 22-23 as modified with Leser).

Regarding **Claim 25**, the rejection of claim 21 is incorporated and Serbinis further discloses wherein the method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy (See Column 7, lines 54-57, Column 10, lines 59-64 and also Column 3, lines 16-27).

Regarding **Claim 26**, the rejection of claim 21 is incorporated and Serbinis further discloses evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document (see Column 7, lines 63-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435